UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,011	11/03/2003	Ralph E. Wesinger JR.	GRAPH-003COD	5849

28661 7590 08/13/2008

LEWIS AND ROCA LLP
1663 Hwy 395, Suite 201
Minden, NV 89423

EXAMINER	
TRUVAN, LEYNNA THANH	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
08/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/701,011	WESINGER ET AL	
	Examiner	Art Unit	
	Leynna T. Truvan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-38* is/are pending in the application.

4a) Of the above claim(s) *1-19* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 20-38 remain pending.

Claims 1-19 are cancelled.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/7/2008 has been entered.

Response to Arguments

3. Applicant's arguments with respect to claims 20-38 have been considered but are moot in view of the new ground(s) of rejection.

Examiner traverses the argument on pg.10 (1st paragraph), that Baehr's screen (or firewall) is not intended to facilitate fully bi-directional communications with outside networks. Baehr teaches an invention comprising different connections from different networks via standard network interfaces to the firewall (col.3, lines 36-62). Baehr discusses packets are transmitted from either of the networks via a connection and that domains may communicate with one another through a screen (firewall). Baehr also discusses the communication in question are between a single public network and a single private network and may equally well be applied to multiple private networks connected via a screen to multiple public networks. Hence, Baehr reads on the claimed through which a fully bi-

directional connection may be made between the first and second networks through the firewall (col.3, lines 36-40 and col.5, lines 40-48). Thus, the fully bi-directional communications is with outside networks since the connection may be with a public network where public network is can be given as an outside network.

Examiner traverses the argument on pg.10 (2nd paragraph), that the screening system virtual host does not appear as a "distinct home through which a connection can be made". As established in prior office actions, the claimed virtual host corresponding to a distinct home is given with the specification (pg.16) in mind is where each virtual host relates to a real host or an actual host (home) of one of the networks. Thus, for purposes of applying art, the virtual host specific or distinct to its actual host (home) is one in the same when being referenced to for connection between the networks. The virtual host is not a firewall or a distinct home. The claimed invention merely recites "a multi-homed firewall comprising...virtual hosts of corresponding to a distinct home" where this is given as Baehr's screen having multiple virtual hosts corresponding to an actual host between two networks. And the claimed "through which a fully bi-directional connection may be made between the first and second networks through the firewall" have been addressed above (col.3, lines 36-40 and col.5, lines 40-48). Therefore, Baehr discloses and suggests the claimed invention.

Civanlar is now brought forth to modify the Baehr and Rosotoker combination to teach the obviousness of the claimed each of said virtual hosts corresponding to a distinct home through which a connection may be made. It would have been obvious for a person of ordinary skills in the art to combine the teaching of Baehr with Civanlar to teach each virtual host name corresponds to a particular server that corresponds to the address to a distinct actual server because the mapping of

each server to its arbitrary names ultimately translates into a designation of the actual server to allow connection (Civanlar-col.1, line 63 – col.2, line 7 and col.4, lines 40-51).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 20-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baehr, et al. (US 5,802,320) in view of Rosotoker, et al. (US 5,708,659), and further in view of Civanlar, et al. (US 5,617,540).

As per claim 20:

Baehr discloses a load-sharing server multi-homed firewall array comprising:

an array of firewall machines coupled in parallel with an *[IP-compliant network]*; ***(col.2, lines 8-15 and col.3, lines 15-22 and 50-67)***

each of the firewall machines of the array further comprising:

a first edge connection corresponding to a first network connection and a second edge connection corresponding to a second network connection; ***(col.3, lines 36-62 and Figs.5 and 8)***

said first edge and second edge connection further comprising a first and second set of virtual hosts, said first set of virtual hosts *[configured to interface an associated firewall machine with said*

IP-compliant network] and said second set of virtual hosts configured to interface an associated firewall machine with a private network; ***(col.4, lines 25-50 and col.8, lines 40-45)***

each of said virtual hosts of said first and second set corresponding to a distinct home ***(Fig.6 and col.4, lines 32-37 and 49-51)*** through which a fully bi-directional connection **(col.3, lines 36-40 and col.5, lines 40-48)** may be made between said [*IP-compliant network*] and said private network; ***(col.5, lines 30-52 and col.10, lines 7-31)***

DNS functionality associated with each of firewall machines of the array; ***(col.6, lines 5-10 and 58-67)***

a master configuration file associated with each of the firewall machines; and ***(col.6, lines 30-55 and col.8, lines 12-27)***

wherein an ensuing connection request is mapped to the first firewall machine of the array to respond to a DNS request associated with said ensuing connection request. ***(col.7, lines 28-34 and col.8, line 58 – col.9, line 5))***

According to the applicant's specification (pg.16) that each virtual host corresponds to a "home" (i.e. site) via connection made between the two networks and that homes are synonymous to virtual hosts. So with the specification in mind, Examiner broadly interprets for each of the virtual hosts corresponding to a distinct home is where each virtual host relates to a real host or an actual host (home) of one of the networks. Thus, for purposes of applying art, the virtual host specific or distinct to its actual host (home) is one in the same when being referenced to for connection between the networks.

Baehr discloses that the private network includes hosts and a proxy network includes a proxy virtual host mirroring each of a subset (or all) of the hosts (col.4, lines 25-50). Baehr's proxy hosts or servers are referring to the claimed virtual hosts. According to Baehr, each of the proxy host of the

proxy network corresponds to one of the actual hosts within the private network (col.4, lines 31-39 and 49-50). Thus, Baehr obviously suggests an actual host of the private network is the claimed distinct home and that each proxy host amongst the set of virtual hosts corresponds to a distinct host (home) between the first and second networks through the firewall (col.4, lines 33-37 and Fig.8).

Baehr teaches an invention comprising the private network coupled via a standard network interface to the screening system, the public network is coupled to the screen via another network interface, and the proxy network is coupled to the screen via the network interface (Fig.5 and 8 and col.5, lines 35-41). Based on the information from the packet would indicate the state of the connection to a particular host or service in the network (col.6, lines 44-45) and such information determines whether the source host is in the expected domain (col.6, lines 48-53). The domains communicate with one another through a screen or a conventional firewall via a connection (col.5, lines 45-47). Baehr discloses a screening system which is configured to handle all of the conventional firewall functions plus the screening functions and different connections from different networks via standard network interfaces to the firewall (col.3, lines 36-62). Baehr discloses the claimed edge connection corresponding to a network connection as a port or network interface that is provided for each of the two networks and one or more ports are provided to one or more proxy networks (col.2, lines 8-15). Hence, Bear reads on the claimed multi-homed firewall. Baehr also discusses packets are transmitted from either of the networks via a connection and that domains may communicate with one another through a screen (firewall). Thus, reads on the claimed through which a fully bi-directional connection may be made between the first and second networks through the firewall (col.3, lines 36-40 and col.5, lines 40-48).

Referring to Fig. 5 and 8, shows the private network 330 coupled via a network interface 410 to the screening system, the private network 335 coupled via a network interface 415 to the screening system, and the proxy network 430 is coupled to the screen via the network interface 420 (col.3, lines 36-62 and col.5, lines 35-41). Baehr includes two private networks 330 and 335 with different connections wherein the private network 330 can assume to be the first network (i.e. a corporate domain corp.sun.com – col.5, lines 43-47) and the private network 335 refers to the second network (i.e. an engineering domain eng.sun.com – col.5, lines 39-42). Baehr further discloses the proxy network includes proxies (virtual hosts) for both the eng.sun.com and corp.sun.com (col.5, lines 50-52). Thus, suggests the two different private networks include their own set of virtual proxy hosts. The claimed first edge connection corresponding to the first network connection can be the network interface connecting to a corresponding private network 335. The claimed second edge connection corresponding to first network connection can be the second network interface connecting to the second private network 330. Thus, obviously suggests a first edge connection comprising a first set of virtual hosts for processing connection requests from a first network and a second edge connection comprising a second set of virtual hosts for processing connection requests from a second network (col.5, lines 50-52 and Fig.8). Although, Baehr discloses virtual hosts and ensuing connection request is mapped to the firewall machine of the array to respond to a DNS request associated with said ensuing connection request (col.6, lines 5-62 and col.7, lines 28-34). However, the connection request does not involve an IP-compliant network and a private network through which a connection may be made between said IP-compliant network and said private network.

Rosotoker discloses network technology has suffered from limitations resulting from a proliferation of non-standard protocols, and limitations due to the nature of the protocols and

transmission schemes, which are employed (col.2, lines 22-26). Rosotoker discloses that under heavy traffic, any attempt to determine to which port a packet must be switched must be accomplished speedily to avoid slowing throughput of the network (col.2, lines 41-45). Rosotoker discusses the network protocol processing system interconnection comprises packet conversion logic for conversion between network protocol (col.4, line 66 – col.5, line 1) where the invention is not necessarily limited to the particular protocols and standards used (col.25, lines 45-52). Rosotoker discusses the remote node connections typically exchange packets of data in Novell IPX, Microsoft NetBEUI, or Internet IP format (col.7, lines 65-67). Thus, depending upon the protocol employed internally the data received over a particular port may require translation from one protocol to another (col.18, lines 5-10) obviously suggests the received IP-compliant traffic being destined for said non-IP compliant destination. Further, Rosotoker discloses translating incoming packets in any protocol and outgoing packets in any different protocol (col.9, lines 28-31). Rosotoker discusses the ATM protocol is preferred but can use other protocols (col.8, lines 55-58). Rosotoker teaches the conversion between a network protocol (i.e. IP-compliant) and the data protocol (i.e. non-IP compliant) used to handle large data streams such as MPEG packets but not limited to these particular protocols (col.25, lines 44-53). By translating outgoing packets in any protocol obviously can transform the IP-compliant traffic into a non-IP protocol appropriate for a destination. Hence, Rosotoker obviously suggests an IP-compliant network and a private network through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Baehr teaching network connectivity by allowing connections to be established with the virtual hosts with Rosotoker to teach translation/conversion from one protocol to another (Rosotoker - col.18, lines 5-10) through which a connection may be made between said IP-compliant network and said private

network because translating to a different protocol can accommodate the data stream of a non-IP compliant destination and providing connections to different network protocols to provide multiple external communication port connections transparent to the destined (Rosotoker-col.25, lines 34-37 and 44-52).

In addition, Baehr and Rosotoker combination did not clearly explain each of said virtual hosts corresponding to a distinct home through which a connection may be made.

Civanlar teaches a pool of multimedia servers (or servers: 305, 307, 309, and 311) that can serve clients (321, 323, 325, 327, 329, 331 and 333) (col.3, lines 63-65). Civanlar explains that servers 305 and 311 are connected to ATM switch 315 whiles servers 307 and 309 are connected to ATM switch 312 (col.4, lines 1-6). Civanlar further discloses a service provider designates the names of servers or virtual hosts names that serve as placeholders which ultimately be translated into a designation or an actual server (col.4, lines 39-45). For example, the server named TANGO, RUBY, and KLEO serves different clients. Hence, obtains the layer-3 address of an actual server that corresponds to the virtual host name (col.4, lines 45-58) where a connection is established for requests to the desired multimedia service (col.6, lines 1-16). This is to minimize the geographic disparity between clients and server and maximizing the performance through the network (col.5, lines 1-35). Civanlar further discloses connecting to the name server and requesting the address of a specific server 311 that corresponds with the specific virtual named server TANGO for connection to server 311 (col.7, lines 10-14). Hence, Civanlar obviously discloses that each (virtual host) server with a specific virtual named corresponds to the address of an actual (distinct home) multimedia server (col.4, lines 56-58) reads on the limitation of each of said virtual hosts corresponding to a distinct home through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Baehr with Civanlar to teach each virtual host name corresponds to a particular server that corresponds to the address to a distinct actual server because the mapping of each server to its arbitrary names ultimately translates into a designation of the actual server to allow connection (Civanlar-col.1, line 63 – col.2, line 7 and col.4, lines 40-51).

As per claim 21: See Baehr on col.6, lines 5-10 and 58-67 and col.7, lines 28-34; discussing load-sharing multi-homed firewall array of claim 20, wherein a connection request received from the IP-compliant network is mapped to said first set of virtual hosts on the first firewall machine of the array to respond to a DNS request.

As per claim 22: See Baehr on col.6, lines 5-10 and 58-67 and col.7, lines 28-34;; discussing load-sharing multi-homed firewall array of claim 20, wherein a connection request received from the private network is mapped to said second set of virtual hosts on the first firewall machine of the array to respond to a DNS request.

As per claim 23: See Baehr on col.5, lines 30-35 and col.6, lines 18-25 and col.10, lines 7-31; discussing load-sharing multi-homed firewall array of claim 20, wherein each of said firewall machines further comprises a special-purpose virtual host including an HTML-based configuration module for updating said master configuration files over said IP-compliant network.

As per claim 24: See Baehr on col.4, lines 25-50 and col.8, lines 40-45 and; discussing load-sharing multi-homed firewall array of claim 23, wherein each of said firewall machines includes N + 1 sets of virtual hosts.

As per claim 25:

Baehr discloses a load-sharing multi-homed firewall array comprising:

means for coupling a plurality of firewall means in parallel with *[an IP-compliant network]*; ***(col.2, lines 8-15 and col.3, lines 15-22 and 50-67)***

each of the firewall machines of the array further comprising:

a first edge connection means corresponding to a first network connection and a second edge connection means corresponding to a second network connection; ***(col.3, lines 36-62 and Figs.5 and 8)***

said first edge and second edge connection means further comprising a first set of virtual host means interfacing an associated firewall means [*with said IP-compliant network*] and said second set of virtual host means interfacing an associated firewall means with a private network; ***(col.4, lines 25-50 and col.8, lines 40-45)***

each of said virtual hosts of said first and second set corresponding to a distinct home ***(Fig.6 and col.4, lines 32-37and 49-51)*** through which a fully bi-directional connection **(col.3, lines 36-40 and col.5, lines 40-48)** may be made *between said* [*IP-compliant network*] and said private network; ***(col.5, lines 30-52 and col.10, lines 7-31)***

means for providing DNS functionality associated with each of firewall means; ***(col.6, lines 5-10 and 58-67)***

master configuration means associated with each of the firewall machines; and ***(col.6, lines 30-55 and col.8, lines 12-27)***

means for mapping an ensuing connection request to the first firewall means to respond to a DNS request associated with said ensuing connection request. ***(col.7, lines 28-34 and col.8, line 58 – col.9, line 5)***

According to the applicant's specification (pg.16) that each virtual host corresponds to a "home" (i.e. site) via connection made between the two networks and that homes are synonymous to virtual hosts. So with the specification in mind, Examiner broadly interprets for each of the virtual

hosts corresponding to a distinct home is where each virtual host relates to a real host or an actual host (home) of one of the networks. Thus, for purposes of applying art, the virtual host specific or distinct to its actual host (home) is one in the same when being referenced to for connection between the networks.

Baehr discloses that the private network includes hosts and a proxy network includes a proxy virtual host mirroring each of a subset (or all) of the hosts (col.4, lines 25-50). Baehr's proxy hosts or servers are referring to the claimed virtual hosts. According to Baehr, each of the proxy host of the proxy network corresponds to one of the actual hosts within the private network (col.4, lines 31-39 and 49-50). Thus, Baehr obviously suggests an actual host of the private network is the claimed distinct home and that each proxy host amongst the set of virtual hosts corresponds to a distinct host (home) between the first and second networks through the firewall (col.4, lines 33-37 and Fig.8).

Baehr teaches an invention comprising the private network coupled via a standard network interface to the screening system, the public network is coupled to the screen via another network interface, and the proxy network is coupled to the screen via the network interface (Fig.5 and 8 and col.5, lines 35-41). Based on the information from the packet would indicate the state of the connection to a particular host or service in the network (col.6, lines 44-45) and such information determines whether the source host is in the expected domain (col.6, lines 48-53). The domains communicate with one another through a screen or a conventional firewall via a connection (col.5, lines 45-47). Baehr discloses a screening system which is configured to handle all of the conventional firewall functions plus the screening functions and different connections from different networks via standard network interfaces to the firewall (col.3, lines 36-62). Baehr discloses the claimed edge connection corresponding to a network connection as a port or network interface that is

provided for each of the two networks and one or more ports are provided to one or more proxy networks (col.2, lines 8-15). Hence, Bear reads on the claimed multi-homed firewall. Baehr also discusses packets are transmitted from either of the networks via a connection and that domains may communicate with one another through a screen (firewall). Thus, reads on the claimed through which a fully bi-directional connection may be made between the first and second networks through the firewall (col.3, lines 36-40 and col.5, lines 40-48).

Referring to Fig. 5 and 8, shows the private network 330 coupled via a network interface 410 to the screening system, the private network 335 coupled via a network interface 415 to the screening system, and the proxy network 430 is coupled to the screen via the network interface 420 (col.3, lines 36-62 and col.5, lines 35-41). Baehr includes two private networks 330 and 335 with different connections wherein the private network 330 can assume to be the first network (i.e. a corporate domain corp.sun.com – col.5, lines 43-47) and the private network 335 refers to the second network (i.e. an engineering domain eng.sun.com – col.5, lines 39-42). Baehr further discloses the proxy network includes proxies (virtual hosts) for both the eng.sun.com and corp.sun.com (col.5, lines 50-52). Thus, suggests the two different private networks include their own set of virtual proxy hosts. The claimed first edge connection corresponding to the first network connection can be the network interface connecting to a corresponding private network 335. The claimed second edge connection corresponding to first network connection can be the second network interface connecting to the second private network 330. Thus, obviously suggests a first edge connection comprising a first set of virtual hosts for processing connection requests from a first network and a second edge connection comprising a second set of virtual hosts for processing connection requests from a second network (col.5, lines 50-52 and Fig.8). Although, Baehr discloses virtual hosts and ensuing connection

request is mapped to the firewall machine of the array to respond to a DNS request associated with said ensuing connection request (col.6, lines 5-62 and col.7, lines 28-34). However, the connection request does not involve an IP-compliant network and a private network through which a connection may be made between said IP-compliant network and said private network.

Rosotoker discloses network technology has suffered from limitations resulting from a proliferation of non-standard protocols, and limitations due to the nature of the protocols and transmission schemes, which are employed (col.2, lines 22-26). Rosotoker discloses that under heavy traffic, any attempt to determine to which port a packet must be switched must be accomplished speedily to avoid slowing throughput of the network (col.2, lines 41-45). Rosotoker discusses the network protocol processing system interconnection comprises packet conversion logic for conversion between network protocol (col.4, line 66 – col.5, line 1) where the invention is not necessarily limited to the particular protocols and standards used (col.25, lines 45-52). Rosotoker discusses the remote node connections typically exchange packets of data in Novell IPX, Microsoft NetBEUI, or Internet IP format (col.7, lines 65-67). Thus, depending upon the protocol employed internally the data received over a particular port may require translation from one protocol to another (col.18, lines 5-10) obviously suggests the received IP-compliant traffic being destined for said non-IP compliant destination. Further, Rosotoker discloses translating incoming packets in any protocol and outgoing packets in any different protocol (col.9, lines 28-31). Rosotoker discusses the ATM protocol is preferred but can use other protocols (col.8, lines 55-58). Rosotoker teaches the conversion between a network protocol (i.e. IP-compliant) and the data protocol (i.e. non-IP compliant) used to handle large data streams such as MPEG packets but not limited to these particular protocols (col.25, lines 44-53). By translating outgoing packets in any protocol obviously can transform the IP-

compliant traffic into a non-IP protocol appropriate for a destination. Hence, Rosotoker obviously suggests an IP-compliant network and a private network through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Baehr teaching network connectivity by allowing connections to be established with the virtual hosts with Rosotoker to teach translation/conversion from one protocol to another (Rosotoker - col.18, lines 5-10) through which a connection may be made between said IP-compliant network and said private network because translating to a different protocol can accommodate the data stream of a non-IP compliant destination and providing connections to different network protocols to provide multiple external communication port connections transparent to the destined (Rosotoker-col.25, lines 34-37 and 44-52).

In addition, Baehr and Rosotoker combination did not clearly explain each of said virtual hosts corresponding to a distinct home through which a connection may be made.

Civanlar teaches a pool of multimedia servers (or servers: 305, 307, 309, and 311) that can serve clients (321, 323, 325, 327, 329, 331 and 333) (col.3, lines 63-65). Civanlar explains that servers 305 and 311 are connected to ATM switch 315 whiles servers 307 and 309 are connected to ATM switch 312 (col.4, lines 1-6). Civanlar further discloses a service provider designates the names of servers or virtual hosts names that serve as placeholders which ultimately be translated into a designation or an actual server (col.4, lines 39-45). For example, the server named TANGO, RUBY, and KLEO serves different clients. Hence, obtains the layer-3 address of an actual server that corresponds to the virtual host name (col.4, lines 45-58) where a connection is established for requests to the desired multimedia service (col.6, lines 1-16). This is to minimize the geographic disparity between clients and server and maximizing the performance through the network (col.5,

lines 1-35). Civanlar further discloses connecting to the name server and requesting the address of a specific server 311 that corresponds with the specific virtual named server TANGO for connection to server 311 (col.7, lines 10-14). Hence, Civanlar obviously discloses that each (virtual host) server with a specific virtual named corresponds to the address of an actual (distinct home) multimedia server (col.4, lines 56-58) reads on the limitation of each of said virtual hosts corresponding to a distinct home through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Baehr with Civanlar to teach each virtual host name corresponds to a particular server that corresponds to the address to a distinct actual server because the mapping of each server to its arbitrary names ultimately translates into a designation of the actual server to allow connection (Civanlar-col.1, line 63 – col.2, line 7 and col.4, lines 40-51).

As per claim 26: See Baehr on col.6, lines 5-10 and 58-67 and col.7, lines 28-34;; discussing load-sharing multi-homed firewall array of claim 25, further comprising means for mapping a connection request received from the IP-compliant network to said first set of virtual host means on the first firewall means to respond to a DNS request.

As per claim 27: See Baehr on col.6, lines 5-10 and 58-67 and col.7, lines 28-34;; discussing load-sharing multi-homed firewall array of claim 25, further comprising means for mapping a connection request received from the private network to said second set of virtual host means on the first firewall means to respond to a DNS request.

As per claim 28: See Baehr on col.5, lines 30-35 and col.6, lines 18-25 and col.10, lines 7-31; discussing load-sharing multi-homed firewall array of claim 25, further comprising HTML-based configuration means for updating said master configuration means over said IP-compliant network.

As per claim 29: See Baehr on col.4, lines 25-50 and col.8, lines 40-45 and; discussing load-sharing multi-homed firewall array of claim 28, wherein each of said firewall means includes N + 1 sets of virtual host means.

As per claim 30:

Baehr discloses a load-sharing multi-homed firewall array comprising:

an array of firewall machines coupled in a parallel with an [IP-compliant network]; ***(col.2, lines 8-15 and col.3, lines 15-22 and 50-67)***

each of the firewall machines of the array further comprising:

a first edge connection corresponding to a first network connection and a second edge connection corresponding to a second network connection; ***(col.3, lines 36-62 and Figs.5 and 8)***

said first edge and second edge connection further comprising at least a first and second set of virtual hosts, said first set of virtual hosts ***(Fig.6)*** *[configured to interface an associated firewall machine with said IP-compliant network]* and said second set of virtual hosts configured to interface an associated firewall machine with a private network; ***(col.4, lines 25-50 and col.8, lines 40-45)***

each of said virtual hosts of said first and second sets corresponding to a distinct home ***(Fig.6 and col.4, lines 32-37 and 49-51)*** through which a fully bi-directional connection may be made between *[said IP-compliant network]* and said private network; ***(col.3, lines 36-40 and col.5, lines 40-48)***

DNS functionality associated with each of firewall machines of the array; ***(col.6, lines 5-10 and 58-67)***

a master configuration file associated with each of the firewall machines; ***(col.6, lines 30-51 and col.8, lines 12-27)***

a special-purpose virtual host including an HTML-based configuration module for updating said master configuration files using a point-and-click interface over said *[IP-compliant network]*; and ***(col.5, lines 30-35 and col.6, lines 18-25 and col.10, lines 7-31)***

wherein an ensuing connection request is mapped to the first firewall machine of the array to respond to a DNS request associated with said ensuing connection request. ***(col.7, lines 28-34 and col.8, line 58 – col.9, line 5)***

According to the applicant's specification (pg.16) that each virtual host corresponds to a "home" (i.e. site) via connection made between the two networks and that homes are synonymous to virtual hosts. So with the specification in mind, Examiner broadly interprets for each of the virtual hosts corresponding to a distinct home is where each virtual host relates to a real host or an actual host (home) of one of the networks. Thus, for purposes of applying art, the virtual host specific or distinct to its actual host (home) is one in the same when being referenced to for connection between the networks.

Baehr discloses that the private network includes hosts and a proxy network includes a proxy virtual host mirroring each of a subset (or all) of the hosts (col.4, lines 25-50). Baehr's proxy hosts or servers are referring to the claimed virtual hosts. According to Baehr, each of the proxy host of the proxy network corresponds to one of the actual hosts within the private network (col.4, lines 31-39 and 49-50). Thus, Baehr obviously suggests an actual host of the private network is the claimed distinct home and that each proxy host amongst the set of virtual hosts corresponds to a distinct host (home) between the first and second networks through the firewall (col.4, lines 33-37 and Fig.8).

Baehr teaches an invention comprising the private network coupled via a standard network interface to the screening system, the public network is coupled to the screen via another network

interface, and the proxy network is coupled to the screen via the network interface (Fig.5 and 8 and col.5, lines 35-41). Based on the information from the packet would indicate the state of the connection to a particular host or service in the network (col.6, lines 44-45) and such information determines whether the source host is in the expected domain (col.6, lines 48-53). The domains communicate with one another through a screen or a conventional firewall via a connection (col.5, lines 45-47). Baehr discloses a screening system which is configured to handle all of the conventional firewall functions plus the screening functions and different connections from different networks via standard network interfaces to the firewall (col.3, lines 36-62). Baehr discloses the claimed edge connection corresponding to a network connection as a port or network interface that is provided for each of the two networks and one or more ports are provided to one or more proxy networks (col.2, lines 8-15). Hence, Bear reads on the claimed multi-homed firewall. Baehr also discusses packets are transmitted from either of the networks via a connection and that domains may communicate with one another through a screen (firewall). Thus, reads on the claimed through which a fully bi-directional connection may be made between the first and second networks through the firewall (col.3, lines 36-40 and col.5, lines 40-48).

Referring to Fig. 5 and 8, shows the private network 330 coupled via a network interface 410 to the screening system, the private network 335 coupled via a network interface 415 to the screening system, and the proxy network 430 is coupled to the screen via the network interface 420 (col.3, lines 36-62 and col.5, lines 35-41). Baehr includes two private networks 330 and 335 with different connections wherein the private network 330 can assume to be the first network (i.e. a corporate domain corp.sun.com – col.5, lines 43-47) and the private network 335 refers to the second network (i.e. an engineering domain eng.sun.com – col.5, lines 39-42). Baehr further discloses the proxy

network includes proxies (virtual hosts) for both the eng.sun.com and corp.sun.com (col.5, lines 50-52). Thus, suggests the two different private networks include their own set of virtual proxy hosts. The claimed first edge connection corresponding to the first network connection can be the network interface connecting to a corresponding private network 335. The claimed second edge connection corresponding to first network connection can be the second network interface connecting to the second private network 330. Thus, obviously suggests a first edge connection comprising a first set of virtual hosts for processing connection requests from a first network and a second edge connection comprising a second set of virtual hosts for processing connection requests from a second network (col.5, lines 50-52 and Fig.8). Although, Baehr discloses virtual hosts and ensuing connection request is mapped to the firewall machine of the array to respond to a DNS request associated with said ensuing connection request (col.6, lines 5-62 and col.7, lines 28-34). However, the connection request does not involve an IP-compliant network and a private network through which a connection may be made between said IP-compliant network and said private network.

Rosotoker discloses network technology has suffered from limitations resulting from a proliferation of non-standard protocols, and limitations due to the nature of the protocols and transmission schemes, which are employed (col.2, lines 22-26). Rosotoker discloses that under heavy traffic, any attempt to determine to which port a packet must be switched must be accomplished speedily to avoid slowing throughput of the network (col.2, lines 41-45). Rosotoker discusses the network protocol processing system interconnection comprises packet conversion logic for conversion between network protocol (col.4, line 66 – col.5, line 1) where the invention is not necessarily limited to the particular protocols and standards used (col.25, lines 45-52). Rosotoker discusses the remote node connections typically exchange packets of data in Novell IPX, Microsoft

NetBEUI, or Internet IP format (col.7, lines 65-67). Thus, depending upon the protocol employed internally the data received over a particular port may require translation from one protocol to another (col.18, lines 5-10) obviously suggests the received IP-compliant traffic being destined for said non-IP compliant destination. Further, Rosotoker discloses translating incoming packets in any protocol and outgoing packets in any different protocol (col.9, lines 28-31). Rosotoker discusses the ATM protocol is preferred but can use other protocols (col.8, lines 55-58). Rosotoker teaches the conversion between a network protocol (i.e. IP-compliant) and the data protocol (i.e. non-IP compliant) used to handle large data streams such as MPEG packets but not limited to these particular protocols (col.25, lines 44-53). By translating outgoing packets in any protocol obviously can transform the IP-compliant traffic into a non-IP protocol appropriate for a destination. Hence, Rosotoker obviously suggests an IP-compliant network and a private network through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Baehr teaching network connectivity by allowing connections to be established with the virtual hosts with Rosotoker to teach translation/conversion from one protocol to another (Rosotoker - col.18, lines 5-10) through which a connection may be made between said IP-compliant network and said private network because translating to a different protocol can accommodate the data stream of a non-IP compliant destination and providing connections to different network protocols to provide multiple external communication port connections transparent to the destined (Rosotoker-col.25, lines 34-37 and 44-52).

In addition, Baehr and Rosotoker combination did not clearly explain each of said virtual hosts corresponding to a distinct home through which a connection may be made.

Civanlar teaches a pool of multimedia servers (or servers: 305, 307, 309, and 311) that can serve clients (321, 323, 325, 327, 329, 331 and 333) (col.3, lines 63-65). Civanlar explains that servers 305 and 311 are connected to ATM switch 315 whiles servers 307 and 309 are connected to ATM switch 312 (col.4, lines 1-6). Civanlar further discloses a service provider designates the names of servers or virtual hosts names that serve as placeholders which ultimately be translated into a designation or an actual server (col.4, lines 39-45). For example, the server named TANGO, RUBY, and KLEO serves different clients. Hence, obtains the layer-3 address of an actual server that corresponds to the virtual host name (col.4, lines 45-58) where a connection is established for requests to the desired multimedia service (col.6, lines 1-16). This is to minimize the geographic disparity between clients and server and maximizing the performance through the network (col.5, lines 1-35). Civanlar further discloses connecting to the name server and requesting the address of a specific server 311 that corresponds with the specific virtual named server TANGO for connection to server 311 (col.7, lines 10-14). Hence, Civanlar obviously discloses that each (virtual host) server with a specific virtual named corresponds to the address of an actual (distinct home) multimedia server (col.4, lines 56-58) reads on the limitation of each of said virtual hosts corresponding to a distinct home through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Baehr with Civanlar to teach each virtual host name corresponds to a particular server that corresponds to the address to a distinct actual server because the mapping of each server to its arbitrary names ultimately translates into a designation of the actual server to allow connection (Civanlar-col.1, line 63 – col.2, line 7 and col.4, lines 40-51).

As per claim 31: See Baehr on col.6, lines 5-10 and 58-67 and col.7, lines 28-34; discussing load-sharing multi-homed firewall array of claim 30, wherein: connection request received from the IP-compliant network is mapped to said first set of virtual hosts on the first firewall machine of the array to respond to a DNS request.

As per claim 32: See Baehr on col.6, lines 5-10 and 58-67 and col.7, lines 28-34; discussing load-sharing multi-homed firewall array of claim 30, wherein connection request received from the private network is mapped to said second set of virtual hosts on the first firewall machine of the array to respond to a DNS request.

As per claim 33: See Baehr on col.5, lines 30-35 and col.6, lines 18-25 and col.10, lines 7-31; discussing load-sharing multi-homed firewall array of claim 30, wherein each of said firewall machines further comprises a special-purpose virtual host including an HTML-based configuration module for updating said master configuration files over said IP-compliant network.

As per claim 34: See Baehr on col.4, lines 25-50 and col.8, lines 40-45; discussing load-sharing multi-homed firewall array of claim 33, wherein each of said firewall machines includes N + 1 sets of virtual hosts.

As per claim 35:

Baehr discloses a load-sharing multi-homed firewall array comprising:

means for coupling a plurality of firewall means in parallel with *[an IP-compliant network]*; ***(col.2, lines 8-15 and col.3, lines 15-22 and 50-67)***

each of the firewall machines of the array further comprising:

first edge connection means corresponding to a first network connection and a second edge connection means corresponding to a second network connection; ***(col.3, lines 36-62 and Figs.5 and 8)***

said first edge and second edge connection means further comprising a first set of virtual host means interfacing an associated firewall means ***(Fig.6)*** [*with said IP-compliant network*] and said second set of virtual host means interfacing an associated firewall machine with a private network; ***(col.4, lines 25-50 and col.8, lines 40-45)***

each of said virtual hosts of said first and second sets corresponding to a distinct home ***(Fig.6 and col.4, lines 32-37 and 49-51)*** through which a fully bi-directional connection may be made between said IP-compliant network and said private network; ***(col.3, lines 36-40 and col.5, lines 40-48)***

means for providing DNS functionality associated with each of firewall means; ***(col.6, lines 5-10 and 58-67)***

master configuration means associated with each of the firewall machines; ***(col.6, lines 30-51 and col.8, lines 12-27)***

an HTML-based configuration means for updating said master configuration means using a point-and-click interface over said *[IP-compliant network]*; and ***(col.5, lines 30-35 and col.6, lines 18-25 and col.10, lines 7-31)***

means for mapping an ensuing connection request to the first firewall means to respond to a DNS request associated with said ensuing connection request. ***(col.7, lines 28-34 and col.8, line 58 – col.9, line 5)***

According to the applicant's specification (pg.16) that each virtual host corresponds to a "home" (i.e. site) via connection made between the two networks and that homes are synonymous to virtual hosts. So with the specification in mind, Examiner broadly interprets for each of the virtual hosts corresponding to a distinct home is where each virtual host relates to a real host or an actual host (home) of one of the networks. Thus, for purposes of applying art, the virtual host specific or

distinct to its actual host (home) is one in the same when being referenced to for connection between the networks.

Baehr discloses that the private network includes hosts and a proxy network includes a proxy virtual host mirroring each of a subset (or all) of the hosts (col.4, lines 25-50). Baehr's proxy hosts or servers are referring to the claimed virtual hosts. According to Baehr, each of the proxy host of the proxy network corresponds to one of the actual hosts within the private network (col.4, lines 31-39 and 49-50). Thus, Baehr obviously suggests an actual host of the private network is the claimed distinct home and that each proxy host amongst the set of virtual hosts corresponds to a distinct host (home) between the first and second networks through the firewall (col.4, lines 33-37 and Fig.8).

Baehr teaches an invention comprising the private network coupled via a standard network interface to the screening system, the public network is coupled to the screen via another network interface, and the proxy network is coupled to the screen via the network interface (Fig.5 and 8 and col.5, lines 35-41). Based on the information from the packet would indicate the state of the connection to a particular host or service in the network (col.6, lines 44-45) and such information determines whether the source host is in the expected domain (col.6, lines 48-53). The domains communicate with one another through a screen or a conventional firewall via a connection (col.5, lines 45-47). Baehr discloses a screening system which is configured to handle all of the conventional firewall functions plus the screening functions and different connections from different networks via standard network interfaces to the firewall (col.3, lines 36-62). Baehr discloses the claimed edge connection corresponding to a network connection as a port or network interface that is provided for each of the two networks and one or more ports are provided to one or more proxy networks (col.2, lines 8-15). Hence, Bear reads on the claimed multi-homed firewall. Baehr also

discusses packets are transmitted from either of the networks via a connection and that domains may communicate with one another through a screen (firewall). Thus, reads on the claimed through which a fully bi-directional connection may be made between the first and second networks through the firewall (col.3, lines 36-40 and col.5, lines 40-48).

Referring to Fig. 5 and 8, shows the private network 330 coupled via a network interface 410 to the screening system, the private network 335 coupled via a network interface 415 to the screening system, and the proxy network 430 is coupled to the screen via the network interface 420 (col.3, lines 36-62 and col.5, lines 35-41). Baehr includes two private networks 330 and 335 with different connections wherein the private network 330 can assume to be the first network (i.e. a corporate domain corp.sun.com – col.5, lines 43-47) and the private network 335 refers to the second network (i.e. an engineering domain eng.sun.com – col.5, lines 39-42). Baehr further discloses the proxy network includes proxies (virtual hosts) for both the eng.sun.com and corp.sun.com (col.5, lines 50-52). Thus, suggests the two different private networks include their own set of virtual proxy hosts. The claimed first edge connection corresponding to the first network connection can be the network interface connecting to a corresponding private network 335. The claimed second edge connection corresponding to first network connection can be the second network interface connecting to the second private network 330. Thus, obviously suggests a first edge connection comprising a first set of virtual hosts for processing connection requests from a first network and a second edge connection comprising a second set of virtual hosts for processing connection requests from a second network (col.5, lines 50-52 and Fig.8). Although, Baehr discloses virtual hosts and ensuing connection request is mapped to the firewall machine of the array to respond to a DNS request associated with said ensuing connection request (col.6, lines 5-62 and col.7, lines 28-34). However, the connection

request does not involve an IP-compliant network and a private network through which a connection may be made between said IP-compliant network and said private network.

Rosotoker discloses network technology has suffered from limitations resulting from a proliferation of non-standard protocols, and limitations due to the nature of the protocols and transmission schemes, which are employed (col.2, lines 22-26). Rosotoker discloses that under heavy traffic, any attempt to determine to which port a packet must be switched must be accomplished speedily to avoid slowing throughput of the network (col.2, lines 41-45). Rosotoker discusses the network protocol processing system interconnection comprises packet conversion logic for conversion between network protocol (col.4, line 66 – col.5, line 1) where the invention is not necessarily limited to the particular protocols and standards used (col.25, lines 45-52). Rosotoker discusses the remote node connections typically exchange packets of data in Novell IPX, Microsoft NetBEUI, or Internet IP format (col.7, lines 65-67). Thus, depending upon the protocol employed internally the data received over a particular port may require translation from one protocol to another (col.18, lines 5-10) obviously suggests the received IP-compliant traffic being destined for said non-IP compliant destination. Further, Rosotoker discloses translating incoming packets in any protocol and outgoing packets in any different protocol (col.9, lines 28-31). Rosotoker discusses the ATM protocol is preferred but can use other protocols (col.8, lines 55-58). Rosotoker teaches the conversion between a network protocol (i.e. IP-compliant) and the data protocol (i.e. non-IP compliant) used to handle large data streams such as MPEG packets but not limited to these particular protocols (col.25, lines 44-53). By translating outgoing packets in any protocol obviously can transform the IP-compliant traffic into a non-IP protocol appropriate for a destination. Hence, Rosotoker obviously suggests an IP-compliant network and a private network through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Baehr teaching network connectivity by allowing connections to be established with the virtual hosts with Rosotoker to teach translation/conversion from one protocol to another (Rosotoker - col.18, lines 5-10) through which a connection may be made between said IP-compliant network and said private network because translating to a different protocol can accommodate the data stream of a non-IP compliant destination and providing connections to different network protocols to provide multiple external communication port connections transparent to the destined (Rosotoker-col.25, lines 34-37 and 44-52).

In addition, Baehr and Rosotoker combination did not clearly explain each of said virtual hosts corresponding to a distinct home through which a connection may be made.

Civanlar teaches a pool of multimedia servers (or servers: 305, 307, 309, and 311) that can serve clients (321, 323, 325, 327, 329, 331 and 333) (col.3, lines 63-65). Civanlar explains that servers 305 and 311 are connected to ATM switch 315 whiles servers 307 and 309 are connected to ATM switch 312 (col.4, lines 1-6). Civanlar further discloses a service provider designates the names of servers or virtual hosts names that serve as placeholders which ultimately be translated into a designation or an actual server (col.4, lines 39-45). For example, the server named TANGO, RUBY, and KLEO serves different clients. Hence, obtains the layer-3 address of an actual server that corresponds to the virtual host name (col.4, lines 45-58) where a connection is established for requests to the desired multimedia service (col.6, lines 1-16). This is to minimize the geographic disparity between clients and server and maximizing the performance through the network (col.5, lines 1-35). Civanlar further discloses connecting to the name server and requesting the address of a specific server 311 that corresponds with the specific virtual named server TANGO for connection to

server 311 (col.7, lines 10-14). Hence, Civanlar obviously discloses that each (virtual host) server with a specific virtual named corresponds to the address of an actual (distinct home) multimedia server (col.4, lines 56-58) reads on the limitation of each of said virtual hosts corresponding to a distinct home through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Baehr with Civanlar to teach each virtual host name corresponds to a particular server that corresponds to the address to a distinct actual server because the mapping of each server to its arbitrary names ultimately translates into a designation of the actual server to allow connection (Civanlar-col.1, line 63 – col.2, line 7 and col.4, lines 40-51).

As per claim 36: See Baehr on col.6, lines 5-10 and 58-67 and col.7, lines 28-34; discussing load-sharing multi-homed firewall array of claim 35, further comprising means for mapping a connection request received from the IP-compliant network to said first set of virtual host means on the first firewall means to respond to a DNS request.

As per claim 37: See Baehr on col.6, lines 5-10 and 58-67 and col.7, lines 28-34; discussing load-sharing multi-homed firewall array of claim 35, further comprising means for mapping a connection request received from the private network to said second set of virtual host means on the first firewall means to respond to a DNS request.

As per claim 38: See Baehr on col.4, lines 25-50 and col.8, lines 40-45 and; discussing load-sharing multi-homed firewall array of claim 35, wherein each of said firewall means includes N + 1 sets of virtual host means.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2135
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135